

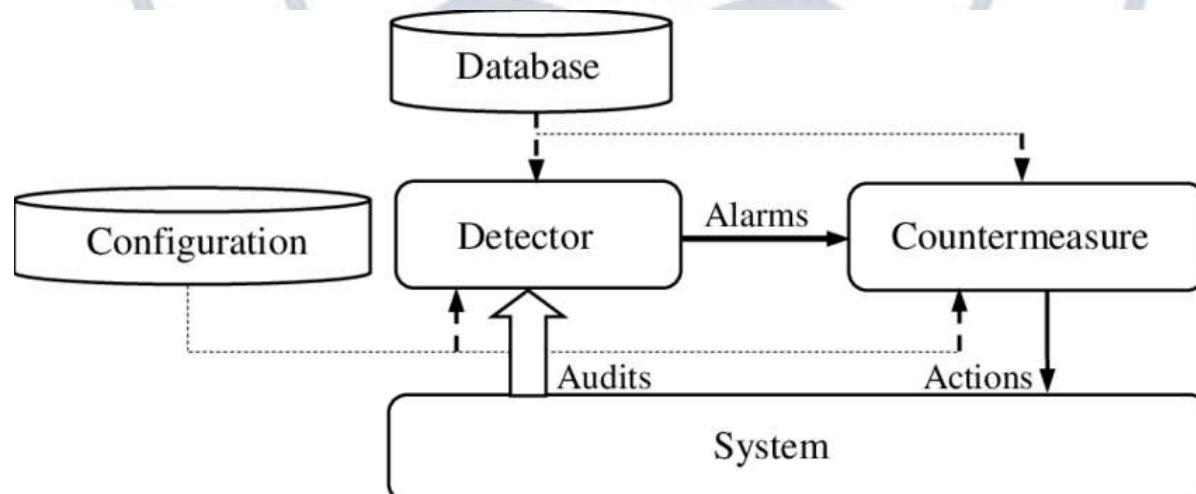
## DEPARTMENT OF COMPUTER APPLICATIONS

### MODULE – 4 : INTRUSION DETECTION

#### Intrusion Detection

##### Introduction

Intrusion Detection is a vital component of cybersecurity that focuses on identifying unauthorized or malicious activities within computer systems and networks. As cyberattacks become more advanced, traditional security mechanisms such as firewalls and antivirus software are no longer sufficient on their own. Intrusion Detection Systems (IDS) monitor system behavior and network traffic to detect suspicious patterns that may indicate security violations. IDS plays a crucial role in protecting sensitive data, maintaining system integrity, and ensuring availability of services. It acts as a second line of defense by alerting administrators when an attack occurs or is attempted. Intrusion detection helps organizations respond quickly to threats, minimize damage, and prevent future attacks. It is widely used in enterprises, government organizations, and critical infrastructure environments.



## DEPARTMENT OF COMPUTER APPLICATIONS

### Explanation

Intrusion Detection Systems are designed to monitor and analyze events occurring in a computer system or network. The main objective is to detect malicious activities or policy violations.

IDS works by collecting data from various sources such as system logs, network packets, and user activities. This data is analyzed using predefined rules or behavioral models. When suspicious activity is detected, the system generates alerts.

There are two primary detection approaches:

- **Signature-based detection**, which compares activity against known attack patterns.
- **Anomaly-based detection**, which identifies deviations from normal behavior.

IDS can detect attacks such as unauthorized access, malware infections, denial-of-service attacks, and insider threats. However, IDS does not block attacks; it only detects and reports them.

Key components of an IDS include:

- Data collection module
- Analysis engine
- Alerting mechanism
- Management console

Advantages of IDS:

- Early attack detection
- Improved incident response
- Compliance support

## DEPARTMENT OF COMPUTER APPLICATIONS

Limitations include false positives, false negatives, and resource consumption. Despite these challenges, IDS remains essential for modern cybersecurity defense strategies.

### Example

An organization installs an IDS to monitor internal network traffic. The IDS detects repeated login failures from a single IP address and raises an alert. Investigation reveals a brute-force password attack, allowing administrators to take immediate action by blocking the IP and securing accounts.

### Conclusion

Intrusion Detection is a fundamental security mechanism that enhances visibility into system and network activities. By detecting malicious behavior early, IDS helps reduce the impact of cyberattacks. Although it does not prevent attacks directly, it significantly strengthens overall security when combined with other defense tools.

### Topic 2: Host-Based Intrusion Detection System (HIDS)

#### Introduction

A Host-Based Intrusion Detection System (HIDS) monitors activities occurring on an individual host or system. It focuses on detecting unauthorized access, file modifications, and abnormal system behavior. HIDS is installed directly on servers, workstations, or endpoints and provides deep visibility into internal operations. This makes it especially effective in detecting insider threats and attacks that bypass network security controls. HIDS plays an important role in protecting critical systems by monitoring logs, system calls, and application activity. It complements network-based detection by focusing on what happens inside the host itself.

## DEPARTMENT OF COMPUTER APPLICATIONS

### Explanation

HIDS monitors and analyzes internal system behavior rather than network traffic. It examines:

- System logs
- File integrity
- User authentication attempts
- Application activity

HIDS uses signature-based and anomaly-based detection techniques. File Integrity Monitoring (FIM) is a key feature, ensuring that critical files are not altered without authorization.

Advantages of HIDS:

- Detects insider threats
- Identifies system-level attacks
- Monitors encrypted traffic (after decryption)

Disadvantages:

- High resource usage
- Limited visibility beyond host
- Requires installation on each system

HIDS is commonly used in servers hosting sensitive data such as databases and financial systems.

### Example

A HIDS detects unauthorized changes to system configuration files on a server. The alert helps administrators identify a compromised user account attempting privilege escalation.



## DEPARTMENT OF COMPUTER APPLICATIONS

### Conclusion

HIDS provides detailed insight into host-level activities and is highly effective against internal threats. When combined with other detection systems, it strengthens endpoint security and improves attack detection accuracy.

### Topic 3: Network-Based Intrusion Detection System (NIDS)

#### Introduction

A Network-Based Intrusion Detection System (NIDS) monitors network traffic to identify suspicious or malicious activities. It is placed at strategic points within the network to analyze packets flowing between devices. NIDS helps detect attacks such as denial-of-service, scanning, and malware propagation. It provides a centralized view of network security and is widely used in enterprise environments.

#### Explanation

NIDS captures and analyzes packets in real time. It examines:

- Packet headers
- Payload data
- Traffic patterns

Detection methods include:

- Signature-based detection
- Anomaly-based detection

Advantages:

## DEPARTMENT OF COMPUTER APPLICATIONS

- Monitors entire network
- No impact on host performance
- Easy centralized management

### Limitations:

- Cannot analyze encrypted traffic
- High traffic volumes can reduce accuracy

NIDS is effective for detecting external threats and large-scale attacks.

### Example

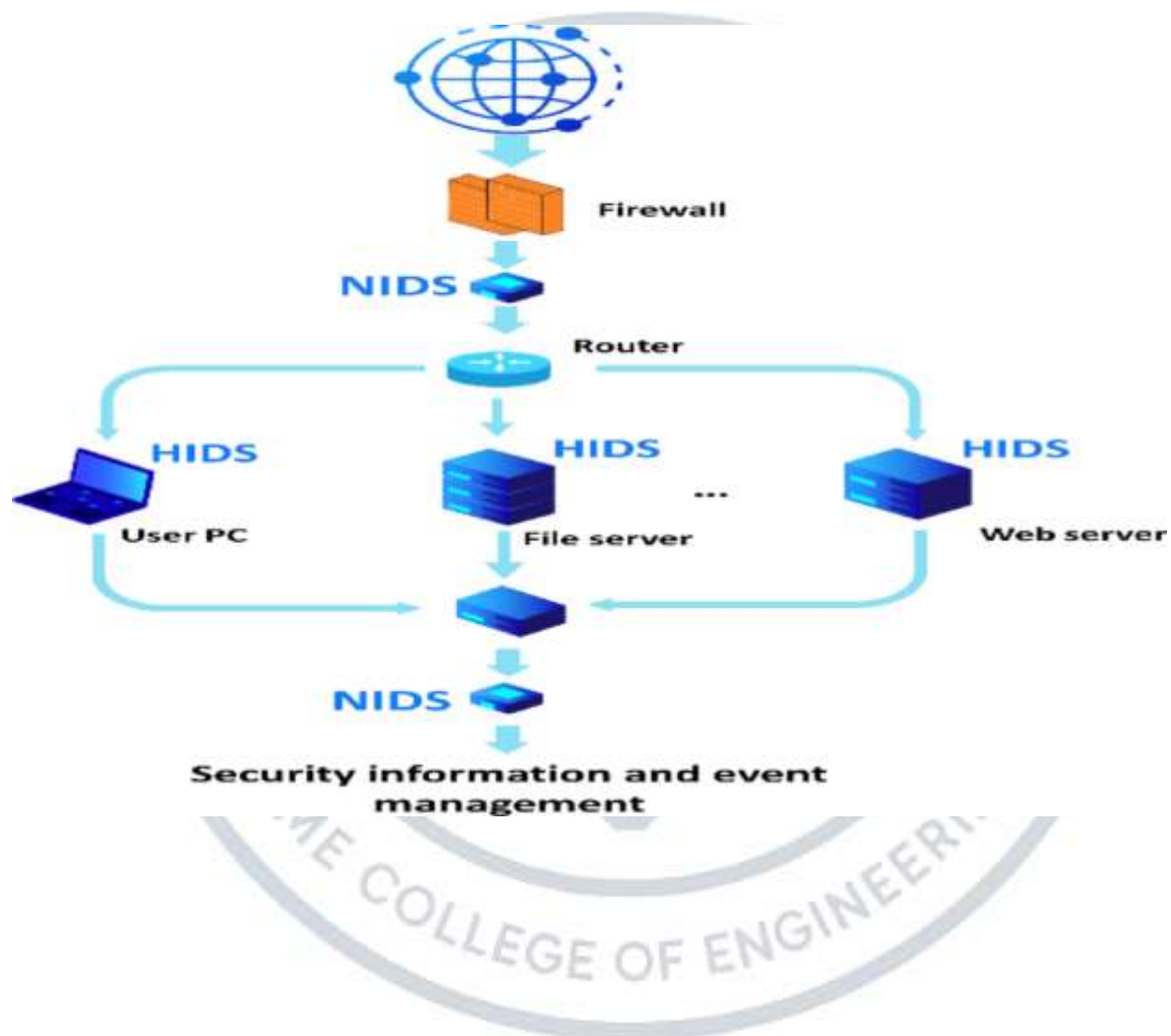
A NIDS detects abnormal traffic spikes targeting a web server and raises an alert, indicating a potential DDoS attack.

### Conclusion

NIDS provides broad visibility into network activities and is essential for detecting external attacks. It is most effective when combined with host-based systems.

## DEPARTMENT OF COMPUTER APPLICATIONS

### Basic architecture and placement of NIDS and HIDS



## DEPARTMENT OF COMPUTER APPLICATIONS

### Topic 4: Distributed or Hybrid Intrusion Detection

#### Introduction

Distributed or Hybrid Intrusion Detection combines multiple IDS components to provide comprehensive security coverage. It integrates host-based and network-based systems to improve detection accuracy. This approach is ideal for large, complex networks.

#### Explanation

Hybrid IDS systems collect data from multiple sources and correlate events. Benefits include:

- Reduced false positives
- Better attack correlation
- Scalability

Challenges include complexity and higher costs.

#### Example

A hybrid IDS correlates suspicious login attempts detected by HIDS with network scanning detected by NIDS, confirming a coordinated attack.

#### Conclusion

Distributed IDS offers enhanced detection capabilities and is suitable for modern enterprise environments.

#### Intrusion Detection Exchange Format (IDXF)



## DEPARTMENT OF COMPUTER APPLICATIONS

### Introduction

IDXF is a standardized format used to share intrusion detection information between systems. It enables interoperability and centralized analysis.

### Explanation

IDXF supports:

- Alert sharing
- Event correlation
- Incident reporting

It improves collaboration among security tools.

### Example

Multiple IDS sensors share alerts using IDXF to detect a multi-stage attack.

### Conclusion

IDXF enhances coordination and effectiveness of intrusion detection systems.

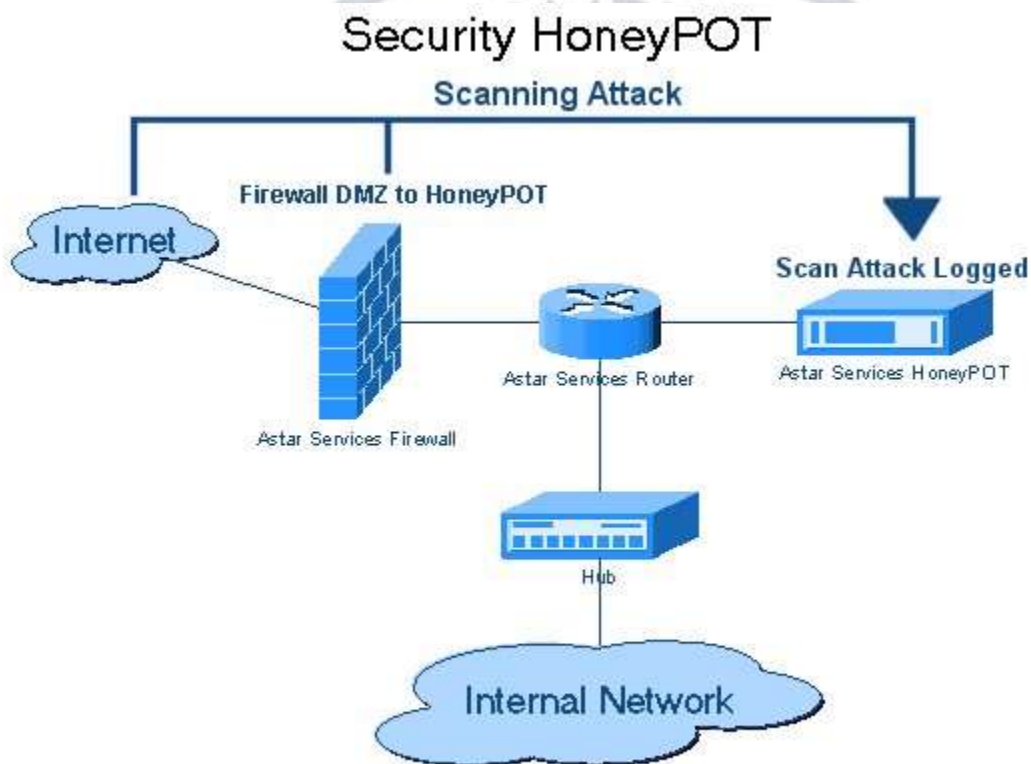
### Topic 6: Honeypots

#### Introduction

A honeypot is a deliberately designed decoy system or network resource created to attract cyber attackers and observe their behavior. Unlike traditional security mechanisms that focus on blocking attacks, honeypots are used to lure attackers so that their methods, tools, and intentions can be studied. A honeypot appears to be a legitimate and vulnerable system, but it is isolated from critical production systems to avoid real damage. Since honeypots have no authorized

## DEPARTMENT OF COMPUTER APPLICATIONS

users, any interaction with them is considered suspicious or malicious by default. Honeypots play an important role in intrusion detection, threat analysis, and cyber forensics. They help security professionals understand new attack techniques and malware behavior. By collecting detailed attack data, honeypots support the development of stronger security policies and defensive strategies. They are widely used in research environments, enterprises, and government security operations to enhance cyber threat intelligence.



## DEPARTMENT OF COMPUTER APPLICATIONS

### Explanation

A honeypot is a controlled security resource whose value lies in being probed, attacked, or compromised. Its primary purpose is not prevention but detection and analysis of malicious activities.

Honeypots are intentionally configured with weaknesses such as open ports, outdated software, or vulnerable services to attract attackers. Once an attacker interacts with the honeypot, all actions are logged and monitored for analysis.

Honeypots are broadly classified into two categories:

#### 1. Low-Interaction Honeypots

These honeypots simulate limited services and interactions. They do not run full operating systems.

- Easy to deploy and maintain
- Low risk of compromise
- Limited information about attacker behavior

#### 2. High-Interaction Honeypots

These are real systems with actual operating systems and services.

- Provide detailed insights into attacker techniques
- Allow observation of malware behavior
- Higher risk if not properly isolated

Based on deployment, honeypots can also be classified as:

## DEPARTMENT OF COMPUTER APPLICATIONS

- **Production Honeypots** – Used in organizations to improve security monitoring
- **Research Honeypots** – Used by researchers to study attack trends

Key characteristics of honeypots include:

- No legitimate traffic
- High-quality attack data
- Controlled and monitored environment

Advantages of honeypots:

- Early detection of unknown attacks
- Reduced false positives
- Improved threat intelligence
- Insight into attacker tools and strategies

Limitations of honeypots:

- Limited visibility (only detect attacks aimed at them)
- Risk of misuse if attackers gain control
- Requires careful monitoring and isolation

Honeypots are often integrated with Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) tools to enhance overall cybersecurity monitoring.

### Example

A cybersecurity team deploys a honeypot server that mimics an outdated web application. An attacker exploits a known vulnerability and uploads malware. The honeypot records every command executed by the attacker, the malware files used, and the IP address involved. Analysis of this data helps the organization identify new attack patterns and strengthen defenses on real



## DEPARTMENT OF COMPUTER APPLICATIONS

servers. Another example is the use of honeypots by security researchers to capture ransomware samples and study encryption techniques used by attackers.

### Conclusion

Honeypots are powerful tools for understanding and analyzing cyber threats rather than directly preventing them. They provide valuable insight into attacker behavior, tools, and vulnerabilities. When properly deployed and monitored, honeypots significantly enhance intrusion detection and threat intelligence capabilities. Despite their limitations, they remain an important component of modern cybersecurity strategies.

### Topic 7: SNORT

#### Introduction

SNORT is a widely used open-source **Network Intrusion Detection System (NIDS)** developed to monitor real-time network traffic and detect malicious activities. It is designed to analyze packets flowing through a network and compare them against a set of predefined rules to identify possible intrusions. SNORT is popular in both academic and industrial environments due to its flexibility, efficiency, and cost-effectiveness. It helps administrators detect attacks such as port scanning, denial-of-service attempts, malware propagation, and suspicious network behavior. SNORT can operate in different modes depending on security requirements, ranging from simple packet sniffing to full intrusion detection. Its rule-based architecture allows customization for specific network environments. Because of its open-source nature, SNORT has a large community contributing rules and updates, making it an effective and continuously evolving security tool.

## DEPARTMENT OF COMPUTER APPLICATIONS

### Explanation

SNORT functions as a lightweight yet powerful intrusion detection and prevention system. It inspects network packets and identifies suspicious activity based on predefined rules.

SNORT operates in **three main modes**:

#### 1. Sniffer Mode

In this mode, SNORT reads network packets and displays them on the console. It is mainly used for troubleshooting and understanding network traffic patterns.

#### 2. Packet Logger Mode

SNORT logs packets to disk for later analysis. This mode is useful for forensic investigations and traffic analysis.

#### 3. Network Intrusion Detection Mode

This is the most important mode, where SNORT analyzes traffic in real time and generates alerts when malicious activity is detected.

### Core Components of SNORT

- **Packet Decoder**  
Captures packets from the network interface and prepares them for analysis.
- **Preprocessors**  
Normalize traffic and detect protocol anomalies before rule matching.
- **Detection Engine**  
Compares packets against a set of rules to identify attacks.

## DEPARTMENT OF COMPUTER APPLICATIONS

- **Logging and Alerting System**

Records alerts and suspicious activity for administrator review.

- **Output Modules**

Store logs in files, databases, or send alerts to external systems.

### SNORT Rules

SNORT uses rule-based detection. Each rule consists of:

- Rule header (action, protocol, source, destination)
- Rule options (content matching, flags, payload inspection)

Example rule concept:

- Detects port scans
- Identifies malicious payload patterns
- Flags unauthorized access attempts

### Advantages of SNORT

- Open-source and free
- Real-time detection capability
- Highly customizable rules
- Lightweight and fast
- Strong community support

### Limitations of SNORT

- Requires skilled configuration
- Generates false positives if rules are poorly defined
- Limited effectiveness against encrypted traffic

## DEPARTMENT OF COMPUTER APPLICATIONS

- No built-in response unless configured with IPS features

SNORT is often integrated with **firewalls, SIEM systems, and intrusion prevention systems** to enhance overall security posture.

### Example

An organization deploys SNORT at the network gateway. SNORT detects repeated connection attempts to multiple ports from a single IP address. The system generates an alert indicating a possible port-scanning attack. The administrator investigates the alert, blocks the malicious IP address using the firewall, and updates SNORT rules to prevent similar future attacks. In another case, SNORT identifies malicious payload signatures related to malware communication, allowing early containment of the infected system.

### Conclusion

SNORT is a powerful and flexible intrusion detection system that plays a crucial role in network security monitoring. Its ability to analyze traffic in real time and detect known attack patterns makes it an essential tool for cybersecurity defense. Although it requires proper configuration and expertise, SNORT remains one of the most effective and widely used IDS solutions in practice.